Information Sharing Environment (ISE) Privacy Guidelines
Implementation Guide and ISE Privacy Guidelines Chart

Implementation Guide	ISE Privacy Guidelines
Overview	
The ISE Privacy Guidelines do more than direct agencies to comply with the law (page 2).	**Section 13.d.(iv)** These Guidelines are intended only to improve the internal management of the Federal Government and are not intended to, and do not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, or entities, its officers, employees, or agencies, or any other person.
The ISE Privacy Guidelines require each agency to designate a senior official as the ISE privacy official, with overall agency-wide responsibility for information privacy issues and for directly overseeing the agency's implementation and compliance with the ISE Privacy Guidelines (page 4).	**Section 12.a.** Each agency's senior official with overall agencywide responsibility for information privacy issues (as designated by statute or executive order, or as otherwise identified in response to OMB Memorandum M-05-08 dated February 11, 2005), shall directly oversee the agency's implementation of and compliance with the Guidelines (the "ISE privacy official").
The ISE Privacy Guidelines require that an agency have a distinct written ISE privacy protection policy (page 7).	**Section 12.d.** *ISE Privacy Protection Policy*. Each agency shall develop and implement a written ISE privacy protection policy that sets forth the mechanisms, policies, and procedures its personnel will follow in implementing these Guidelines.
Agencies will have formulated, either by documenting existing policies that satisfy the ISE Privacy Guidelines provisions and/or developing new policies, a privacy protection policy that complies with the basic privacy protections of the ISE Privacy Guidelines (page 8).	**Section 12.d.** *ISE Privacy Protection Policy*. Each agency shall develop and implement a written ISE privacy protection policy that sets forth the mechanisms, policies, and procedures its personnel will follow in implementing these Guidelines.

Implementation Guide	ISE Privacy Guidelines
Stage I	
Each Federal agency and department shall have a written ISE privacy protection policy (page 11).	**Section 12.d.** ISE Privacy Protection Policy. Each agency shall develop and implement a written ISE privacy protection policy that sets forth the mechanisms, policies, and procedures its personnel will follow in implementing these Guidelines.
Stage I, Step 1	
Identify existing law, Executive Orders, policies, and procedures that apply to protected information that will be available or accessed through the ISE (page 11).	**Section 2.a.** *General*. In the development and use of the ISE, all agencies shall, without exception, comply with the Constitution and all applicable laws and Executive Orders relating to the protected information. **Section 2.b.** *Rules Assessment*. Each agency shall implement an ongoing process for identifying and assessing the laws, Executive Orders, policies, and procedures that apply to the protected information that it will make available or access through the ISE. Each agency shall identify, document, and comply with any legal restrictions applicable to such information.
Stage I, Step 2	
Assess existing laws, Executive Orders, policies, and procedures that apply to protected information that will be available or accessed through the ISE to determine if there are any gaps between existing protections and the protections identified in the ISE Privacy Guidelines (page 11).	**Section 2.b.** *Rules Assessment*. Each agency shall implement an ongoing process for identifying and assessing the laws, Executive Orders, policies, and procedures that apply to the protected information that it will make available or access through the ISE. Each agency shall identify, document, and comply with any legal restrictions applicable to such information. Each agency shall adopt internal policies and procedures requiring it to: (i) only seek or retain protected information that is legally permissible for the agency to seek or retain under the laws, regulations, policies, and Executive Orders applicable to the agency; and (ii) ensure that the protected information that the agency makes available through the ISE has been lawfully obtained by the agency and may be lawfully made available through the ISE.

Implementation Guide	ISE Privacy Guidelines
	Section 2.c. *Changes.* If, as part of its rules assessment process, an agency: (i) identifies an issue that poses a significant risk to information privacy rights or other legal protections, it shall as appropriate develop policies and procedures to provide protections that address that issue; (ii) identifies a restriction on sharing protected information imposed by internal agency policy, that significantly impedes the sharing of terrorism information, homeland security information, or law enforcement information (as defined in Section 13 below) in a manner that does not appear to be required by applicable laws or to protect information privacy rights or provide other legal protections, it shall review the advisability of maintaining such restriction; (iii) identifies a restriction on sharing protected information, other than one imposed by internal agency policy, that significantly impedes the sharing of information in a manner that does not appear to be required to protect information privacy rights or provide other legal protections, it shall review such restriction with the ISE Privacy Guidelines Committee (described in Section 12 below), and if an appropriate internal resolution cannot be developed, bring such restriction to the attention of the Attorney General and the Director of National Intelligence (DNI). The Attorney General and the DNI shall review any such restriction and jointly submit any recommendations for changes to such restriction to the Assistant to the President for Homeland Security and Counterterrorism, the Assistant to the President for National Security Affairs, and the Director of the Office of Management and Budget for further review. **Section 3** Protected information should be shared through the ISE only if it is terrorism information, homeland security information, or law enforcement information (as defined in Section 13). Each agency shall adopt internal policies and procedures requiring it to ensure that the agency's access to and use of protected information available through the ISE is consistent with the authorized purpose of the ISE.

Implementation Guide	ISE Privacy Guidelines
	Section 5 *a. Accuracy.* Each agency shall adopt and implement procedures, as appropriate, to facilitate the prevention, identification, and correction of any errors in protected information with the objective of ensuring that such information is accurate and has not erroneously been shared through the ISE. *b. Notice of Errors.* Each agency, consistent with its legal authorities and mission requirements, shall ensure that when it determines that protected information originating from another agency may be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the individual may be affected, the potential error or deficiency will be communicated in writing to the other agency's ISE privacy official (the ISE privacy officials are described in Section 12 below). *c. Procedures.* Each agency, consistent with its legal authorities and mission requirements, shall adopt and implement policies and procedures with respect to the ISE requiring the agency to: (i) take appropriate steps, when merging protected information about an individual from two or more sources, to ensure that the information is about the same individual; (ii) investigate in a timely manner alleged errors and deficiencies and correct, delete, or refrain from using protected information found to be erroneous or deficient; and (iii) retain protected information only so long as it is relevant and timely for appropriate use by the agency, and update, delete, or refrain from using protected information that is outdated or otherwise irrelevant for such use. **Section 6** Each agency shall use appropriate physical, technical, and administrative measures to safeguard protected information shared through the ISE from unauthorized access, disclosure, modification, use, or destruction. **Section 7** *a. Procedures.* Each agency shall modify existing policies and procedures or adopt new ones as appropriate, requiring the agency to: (i) have and enforce policies for reporting, investigating, and responding to violations of agency policies relating to protected information, including taking appropriate

Implementation Guide	ISE Privacy Guidelines
	action when violations are found; (ii) provide training to personnel authorized to share protected information through the ISE regarding the agency's requirements and policies for collection, use, and disclosure of protected information, and, as appropriate, for reporting violations of agency privacy-protection policies; (iii) cooperate with audits and reviews by officials with responsibility for providing oversight with respect to the ISE; and (iv) designate each agency's ISE privacy official to receive reports (or copies thereof if the agency already has a designated recipient of such reports) regarding alleged errors in protected information that originate from that agency. *b. Audit.* Each agency shall implement adequate review and audit mechanisms to enable the agency's ISE privacy official and other authorized officials to verify that the agency and its personnel are complying with these Guidelines in the development and use of the ISE. **Section 8** To the extent consistent with its legal authorities and mission requirements, each agency shall, with respect to its participation in the development and use of the ISE, put in place internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.
Stage I, Step 3	
Protect privacy rights by documenting that existing laws, Executive Orders, policies, and procedures are in compliance with the ISE Privacy Guidelines or develop and adopt new policies that fill the gap(s) identified in the "assess" section (page 11).	**Section 2.c.** *Changes.* If, as part of its rules assessment process, an agency: (i) identifies an issue that poses a significant risk to information privacy rights or other legal protections, it shall as appropriate develop policies and procedures to provide protections that address that issue; (ii) identifies a restriction on sharing protected information imposed by internal agency policy, that significantly impedes the sharing of terrorism information, homeland security information, or law enforcement information (as defined in Section 13 below) in a manner that does not appear to be required by applicable laws or to protect information privacy rights or provide other legal protections, it shall review

Implementation Guide	ISE Privacy Guidelines
	the advisability of maintaining such restriction; (iii) identifies a restriction on sharing protected information, other than one imposed by internal agency policy, that significantly impedes the sharing of information in a manner that does not appear to be required to protect information privacy rights or provide other legal protections, it shall review such restriction with the ISE Privacy Guidelines Committee (described in Section 12 below), and if an appropriate internal resolution cannot be developed, bring such restriction to the attention of the Attorney General and the Director of National Intelligence (DNI). The Attorney General and the DNI shall review any such restriction and jointly submit any recommendations for changes to such restriction to the Assistant to the President for Homeland Security and Counterterrorism, the Assistant to the President for National Security Affairs, and the Director of the Office of Management and Budget for further review. **Section 3** Protected information should be shared through the ISE only if it is terrorism information, homeland security information, or law enforcement information (as defined in Section 13). Each agency shall adopt internal policies and procedures requiring it to ensure that the agency's access to and use of protected information available through the ISE is consistent with the authorized purpose of the ISE. **Section 5** *a. Accuracy.* Each agency shall adopt and implement procedures, as appropriate, to facilitate the prevention, identification, and correction of any errors in protected information with the objective of ensuring that such information is accurate and has not erroneously been shared through the ISE. *b. Notice of Errors.* Each agency, consistent with its legal authorities and mission requirements, shall ensure that when it determines that protected information originating from another agency may be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the individual may be affected, the potential error or deficiency will be communicated in writing to the other agency's ISE privacy official (the ISE privacy officials are described in Section 12 below).

Implementation Guide	ISE Privacy Guidelines
	c. Procedures. Each agency, consistent with its legal authorities and mission requirements, shall adopt and implement policies and procedures with respect to the ISE requiring the agency to: (i) take appropriate steps, when merging protected information about an individual from two or more sources, to ensure that the information is about the same individual; (ii) investigate in a timely manner alleged errors and deficiencies and correct, delete, or refrain from using protected information found to be erroneous or deficient; and (iii) retain protected information only so long as it is relevant and timely for appropriate use by the agency, and update, delete, or refrain from using protected information that is outdated or otherwise irrelevant for such use. **Section 6** Each agency shall use appropriate physical, technical, and administrative measures to safeguard protected information shared through the ISE from unauthorized access, disclosure, modification, use, or destruction. **Section 7** *a. Procedures.* Each agency shall modify existing policies and procedures or adopt new ones as appropriate, requiring the agency to: (i) have and enforce policies for reporting, investigating, and responding to violations of agency policies relating to protected information, including taking appropriate action when violations are found; (ii) provide training to personnel authorized to share protected information through the ISE regarding the agency's requirements and policies for collection, use, and disclosure of protected information, and, as appropriate, for reporting violations of agency privacy-protection policies; (iii) cooperate with audits and reviews by officials with responsibility for providing oversight with respect to the ISE; and (iv) designate each agency's ISE privacy official to receive reports (or copies thereof if the agency already has a designated recipient of such reports) regarding alleged errors in protected information that originate from that agency.

Implementation Guide	ISE Privacy Guidelines
	b. Audit. Each agency shall implement adequate review and audit mechanisms to enable the agency's ISE privacy official and other authorized officials to verify that the agency and its personnel are complying with these Guidelines in the development and use of the ISE. **Section 8** To the extent consistent with its legal authorities and mission requirements, each agency shall, with respect to its participation in the development and use of the ISE, put in place internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

Implementation Guide	ISE Privacy Guidelines
Stage II, Step 1	
Identify existing and planned systems, sharing arrangements, and "protected information" covered by the ISE Privacy Guidelines (page 18).	**Section 4.a.** *Identification and Prior Review*. In order to facilitate compliance with these Guidelines, particularly Section 2 (Compliance with Laws) and Section 3 (Purpose Specification), each agency shall identify its data holdings that contain protected information to be shared through the ISE, and shall put in place such mechanisms as may be reasonably feasible to ensure that protected information has been reviewed pursuant to these Guidelines before it is made available to the ISE. **Section 4.b.** *Notice Mechanisms.* Consistent with guidance and standards to be issued for the ISE, each agency shall put in place a mechanism for enabling ISE participants to determine the nature of the protected information that the agency is making available to the ISE, so that such participants can handle the information in accordance with applicable legal requirements. Specifically, such a mechanism will, to the extent reasonably feasible and consistent with the agency's legal authorities and mission requirements, allow for ISE participants to determine whether: (i) the information pertains to a United States citizen or lawful permanent resident; (ii) the information is subject to specific information privacy or other similar restrictions on access, use or disclosure, and if so, the nature of such restrictions; and (iii) there are limitations on the reliability or accuracy of the information.
Stage II, Step 2	
Assess identified systems to ensure that the "protected information" covered by the sharing arrangements is handled in a manner consistent with the protections afforded by the ISE Privacy Guidelines (page 18).	**Section 4.b.** *Notice Mechanisms.* Consistent with guidance and standards to be issued for the ISE, each agency shall put in place a mechanism for enabling ISE participants to determine the nature of the protected information that the agency is making available to the ISE, so that such participants can handle the information in accordance with applicable legal requirements. Specifically, such a mechanism will, to the extent reasonably feasible and consistent with the agency's legal authorities and mission requirements, allow for ISE participants to determine whether:

Implementation Guide	ISE Privacy Guidelines
	(i) the information pertains to a United States citizen or lawful permanent resident; (ii) the information is subject to specific information privacy or other similar restrictions on access, use or disclosure, and if so, the nature of such restrictions; and (iii) there are limitations on the reliability or accuracy of the information.
Stage II, Step 3	
Protect those systems/information shared in the ISE through documentation of the agency's actions (page 18).	**Section 7** *a. Procedures.* Each agency shall modify existing policies and procedures or adopt new ones as appropriate, requiring the agency to: (i) have and enforce policies for reporting, investigating, and responding to violations of agency policies relating to protected information, including taking appropriate action when violations are found; (ii) provide training to personnel authorized to share protected information through the ISE regarding the agency's requirements and policies for collection, use, and disclosure of protected information, and, as appropriate, for reporting violations of agency privacy-protection policies; (iii) cooperate with audits and reviews by officials with responsibility for providing oversight with respect to the ISE; and (iv) designate each agency's ISE privacy official to receive reports (or copies thereof if the agency already has a designated recipient of such reports) regarding alleged errors in protected information that originate from that agency. *b. Audit.* Each agency shall implement adequate review and audit mechanisms to enable the agency's ISE privacy official and other authorized officials to verify that the agency and its personnel are complying with these Guidelines in the development and use of the ISE. **Section 9** *a. Execution.* The ISE privacy official shall be responsible for ensuring that protections are implemented as appropriate through efforts such as training, business process changes, and system designs. *b. Training.* Each agency shall develop an ongoing training program in the implementation of these Guidelines, and shall provide such training to agency personnel participating in the development and use of the ISE.

Implementation Guide	ISE Privacy Guidelines
	c. Technology. Where reasonably feasible, and consistent with standards and procedures established for the ISE, each agency shall consider and implement, as appropriate, privacy enhancing technologies including, but not limited to, permissioning systems, hashing, data anonymization, immutable audit logs, and authentication.